Canadian Security Intelligence Service

Backgrounder Series

No. 12
February 2002

Security of Information Act

The Canadian Security Intelligence Service is dedicated to the protection of Canada's national security interests and the safety of Canadians. In order to accomplish this task effectively, it is essential that Canadians understand the Service's mandate. This Backgrounder Series is a cost-effective way to inform the Canadian public about CSIS priorities and functions as well as the context in which a modern security intelligence agency must operate.

Introduction

This Backgrounder will attempt to explain recent changes – including a change of name – to the *Official Secrets Act* so that people who could be subject to the *Act*, particularly due to their current or former employment, are informed about the new provisions of the legislation. The McDonald Commission in 1981 commented that one of the most important pieces of legislation relating to the work of a security service is the *Official Secrets Act* (*OSA*). The Law Reform Commission noted that the *OSA* creates crimes that are among the most serious criminal offences since they 'jeopardize the security and well-being of the whole nation and its inhabitants'.

The Government's *Anti-terrorism Act*, Bill C-36, now C-41 of the Statutes of Canada 2001, received royal assent on December 18, 2001 and came into effect on December 24, 2001.

Bill C-36 is divided into seven parts, as follows:

Part 1: amendments to the Criminal Code (56 pages)
Part 2: amendments to the *Official Secrets Act* (20 pages)
Part 3: amendments to the *Canada Evidence Act* (20 pages)
Part 4: *Proceeds of Crime* (Money Laundering) *and Terrorist Financing Act* (22 pages)
Part 5: amendments to other Acts (including *Access to Information* and *Privacy Acts*, the *Canadian Security Intelligence Service Act*, the *National Defence Act*) (18 pages)
Part 6: *Charities Registration* (Security Information) *Act* (9 pages)
Part 7: Coordinating, Review and Commencement Provisions (37 pages)

Background

The *Official Secrets Act* has over the past 30 years been the subject of consistent criticism and calls for reform.

The first *Official Secrets Act* was passed in Britain in 1889 and enacted almost verbatim in Canada in 1890. The Canadian *Act* was transferred to the first Criminal Code in 1892 where it remained until 1939 when the current *Official Secrets Act* was rapidly passed on the eve of World War II. Since 1939, and until Bill C-36 was recently passed, there have been no major changes to the legislation.

The 1939 *Official Secrets Act* had two main provisions: (i) Section 3, the offence of espionage ('spying') and (ii) Section 4 which prohibited the 'wrongful communication of information' (often referred to as 'leakage'). Since 1939, there have been about two dozen prosecutions, almost all under the espionage section – and only six in the last 40 years. Some of the more celebrated cases, including those which were not prosecuted, were Peter Treu (1978), the Toronto Sun (1979), Hugh Hambleton (1982), James Morrison (1986), Stephen Ratkai (1989), Brian McInnis (1994-95).

Over the past 30 years, interest in improving or replacing the *Act* has varied depending on events surrounding leakage and espionage incidents, prosecutions under the *Act*, recommendations of federal commissions and other related national or international developments.

In 1969, the Royal Commission on Security (the 'Mackenzie Commission') described the *Official Secrets Act* as "an unwieldy statute, couched in very broad and ambiguous language"; the Commission concluded that "consideration should be given to a complete revision of the Canadian *Official Secrets Act*" (*OSA*).

The early 1970s saw many democratic countries grapple with the issue of improved public access to government information. In 1976, the House of Commons referred to a joint standing committee the issues of freedom of information, protection of privacy and the *OSA*. Consideration of the first two subjects would result in legislation (passed in 1983 as the *Access to Information* and *Privacy Acts*) but the third did not receive the same attention.

In 1979, the Commission of Inquiry concerning Certain Activities of the Royal Canadian Mounted Police (the 'McDonald Commission') spent over half of its first report, entitled 'Security and Information' examining and recommending changes to the *Official Secrets Act*. These recommendations were reiterated in the second report of the McDonald Commission published in August 1981, the report which led to the Government's decision to create CSIS. However, amendment of the *Official Secrets Act* was not pursued – despite a general and often-stated recognition of the need for reform.

Finally, in 1986, perhaps the most scathing criticism of the *Official Secrets Act* appeared – in the form of the Law Reform Commission Working Paper 49. The Commission concluded:

> "Not only are the existing offences against the State out of date, complex, repetitive, vague, inconsistent, lacking in principle and overinclusive, but there is reason to suspect that some of the sections offend the provisions of the Canadian Charter of Rights and Freedoms as well."

Issues

Even with all of the criticisms of the *Act*, reform of the *Official Secrets Act* has been recognized as and has proven to be a difficult undertaking.

The **espionage** provisions are perhaps easier to address since they deal with the issue of when a citizen should be held criminally liable for the disclosure of information **to a foreign entity**, when that disclosure somehow puts Canada at risk or creates an advantage for that foreign entity. Related issues include: what kind of information should be covered? who are the 'foreign entities'? what does it mean and how does one prove in a criminal context that the disclosure is 'prejudicial to the safety or interests of the State' (to use the words from former Section 3 of the *OSA*)?

The **leakage** provisions are more problematic since they deal with the disclosure of information not to foreign entities but **to anyone** (e.g. journalists, MPs, interest groups, etc.). The unauthorized release of government information can do the same damage to a nation's sovereignty and the safety of its citizens as can espionage; however, unlike espionage, these issues are not always apparent, and sometimes not even present. Leakage is more likely to be associated with issues such as freedom of speech, keeping government accountable, informing the public of important public policy issues and whistleblowing.

More recently, although again before the events of September 11, 2001 and Bill C-36, there has been a renewed recognition within the Government of the need to examine the *Official Secrets Act*. In his 1998 Statement on National Security to the House of Commons, the (then) Solicitor General Andy Scott stated:

> "As part of our response to foreign-directed and other threats, the government is also reviewing the *Official Secrets Act*. It has been criticized as lacking precision, being overbroad and for failing to meet the national security issues of today. The *Official Secrets Act* is rooted in an outdated concept of national defence and security, primarily associated with physical security and protecting the country against military threats. In today's information age where crime, terrorism and espionage transcend national boundaries, new threats can put Canadian sovereignty at risk. To address the threats that Canada faces today, we need to look to modern legislation that is focussed, clear and which reflects the values of contemporary society."

The new Security of Information Act

Overview

The Government of Canada press release/backgrounder issued on December 18, 2001, the day Bill C-36 received royal assent, contained the following brief description of the amendments to the *OSA*:

> "The *Official Secrets Act* (was) amended to address national security concerns, including threats of espionage by foreign powers and terrorist groups, and the intimidation or coercion of ethnocultural communities in Canada. The *Act* will also have a new title: the *Security of Information Act*.
>
> New offences (were) created to improve and modernize the "spying" provisions of the *Act*, taking into account new realities, including new players and new threats. These offences will focus upon those situations in which it is

appropriate for Canada to protect its institutions and citizenry from information-related conduct that is harmful or likely to be harmful to Canada.

New players (other than the governments of traditional states) include governments-in-waiting, governments in exile and other foreign powers, as well as terrorist groups.

New threats that are being recognized include threats against ethnocultural communities in Canada, threats to trade secrets and threats to essential infrastructures, both public and private.

The *Act* also includes specific new offences dealing with unauthorized communication, or purported communication, of special operational information (for example, the identity of confidential targets, covert agents or targets of CSIS) by persons permanently bound to secrecy."

New definitions and concepts

New players

As noted in the press release/backgrounder, the newly-named *Security of Information Act* includes 'new players'. The old *OSA* created espionage offences that involved disclosure to a 'foreign power' (undefined); the new *Act* contains more precise definitions of 'foreign state', 'foreign power' (broadly defined to include governments of a foreign state, quasi-governments and those who seek to become governments) and 'foreign entity' (defined to include foreign powers, groups of foreign powers or persons acting on their behalf or in association with them). The new *Act* also includes 'terrorist groups', incorporating the definition of that phrase from the recent amendments to the Criminal Code contained in Bill C-36.

Harm to Canadian interests

The old *OSA* created espionage offences where the Crown could prove that disclosure was for 'a **purpose** prejudicial to the safety or interests of the state' (undefined); the new *Security of Information Act*, in subsections 3(1)(a) to (n), defines that phrase in detail – the 13 paragraphs include such matters as:

- committing an offence punishable by two years or more to advance a political, religious or ideological purpose or to benefit a foreign entity or terrorist group
- committing inside or outside of Canada a terrorist activity (importing that definition also from the Criminal Code)
- interfering with a service or system, public or private, that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada (i.e. harming Canada's critical infrastructure)
- impairing the military capability of the Canadian Forces
- impairing or threatening the capabilities of the Government of Canada in relation to security and intelligence
- impairing or threatening the capability to conduct diplomatic relations or international negotiations.

For the purposes of the *Security of Information Act*, harm is caused to Canadian interests if a foreign entity or terrorist group engages in any of these activities.

Safeguarded Information

The new *Act* does not refer to 'classified information': instead it uses the phrase 'information that the Government of Canada or of a province is **taking measures to safeguard**'. The concept here is that in any prosecution, the Crown will have to show that the Government has taken some measures to protect the information. Security classification would presumably be one but not the only way of showing this. For example, if the Director of CSIS tells an employee not to disclose the foreign location of a meeting with a human source, that could (subject to proof in court) be information the Government has 'taken measures to safeguard'. This information would fall within the provisions of the *Security of Information Act* even though it was not contained in a classified document.

Special operational information

This is a new concept which attempts to define the most operationally sensitive kind of Government information: 'special operational information' is defined as information the Government of Canada is 'taking measures to safeguard' that reveals or from which it can be inferred specified sensitive information, including:

- past and current confidential sources of information, intelligence or assistance to the Government of Canada
- places, persons, groups or entities who were, are or are intended to be, targets of covert collection efforts by the Government
- the identity of any person engaged in such covert collection activities
- plans for certain military operations
- the means the Government uses to protect information, including encryption and any vulnerabilities
- similar information to the above that relates to or is received from foreign entities or terrorist groups.

Persons permanently bound to secrecy

Another new concept introduced in the *Act* is the description of individuals who should be held to a higher level of accountability for unauthorized disclosures. Persons can become part of this 'special regime' in two ways: (a) by being current or former employees of particular departments or agencies set out in a schedule to the *Act* or (b) by being personally identified through a notice system set out in the *Act* (and regulations). The former includes:

- current or former employees of CSIS
- current or former employees of the Communications Security Establishment
- former members of employees of the RCMP Security Service and the Communications Branch of the National Research Council
- current or former employees of the Security Intelligence Review Committee and the office of the Inspector General of CSIS
- current or former employees or members of certain groups within the RCMP (e.g. Criminal Intelligence Program, Protective Operations Program).

Offences

Using the above definitions and concepts, the *Security of Information Act* creates a number of offences both with respect to espionage and to leakage. For all of these offences, no prosecutions can be commenced without the consent of the federal Attorney General. A brief description follows, recognizing that these are complicated offences and what follows is only a brief summary. Please refer to the *Act* itself which is available on the CSIS Web site – www.csis-scrs.gc.ca.

Espionage-related

When a person, knowing or being reckless as to whether it is safeguarded information, communicates such information to a foreign entity or terrorist group – and they intend to or are reckless as to whether such disclosure will increase that foreign group's capacity to harm Canadian interests or if actual harm results – that person will be liable to prosecution and imprisonment for life (Section 16). In addition, there is a specific offence, Section 17, dealing with the communication of 'special operational information'. For that offence, no intent to harm is required; simply believing or being reckless as to whether the information disclosed is indeed special operational information is sufficient. Again the penalty could be imprisonment for life.

Another new offence, Section 20, relates to persons who at the direction of a foreign entity or terrorist group induce or attempt to induce any person to do anything that is likely to harm Canadian interests or which is done for the purpose of increasing the capacity of foreigners to harm our interests. Again, the maximum penalty is imprisonment for life.

Another new feature is that 'economic espionage' is included as a crime – fraudulent communication or communication 'without colour of right' of a 'trade secret' (defined) to a 'foreign economic entity' (defined as a foreign state or an 'entity that is controlled in law or fact, or is substantially owned' by a foreign state). Persons convicted are liable to imprisonment for up to 10 years.

Finally, the *Act* sets out a number of 'preparatory acts' for which the penalty is up to two years imprisonment. These can include: (a) entering Canada at the direction of a foreign entity or terrorist group (b) obtaining access to any information (c) knowingly communicating to these foreign groups a willingness to commit the offence (d) possessing any device or software useful for concealing the content of information or for covert communications.

Leakage

The new *Security of Information Act* retains the old offence of unauthorized disclosure (Section 4) from the *OSA*. Most of the new offences relate to 'persons permanently bound to secrecy' – those 'insiders' who are included either because of where they work (e.g. former and current employees of CSIS and CSE) or because they have been personally notified by their Deputy Minister.

For example, Section 13 creates an offence – for which the maximum penalty is 5 years – for those insiders who 'intentionally and without authority, communicate or confirm information that, **if it were true**, would be special operational information'. This offence of **purported** communication recognizes both that (a) insiders are under a special duty with respect to the most sensitive information they had or have access to and (b) that the Crown does not need to prove the truth of the information (since experience has shown that to do so can simply increase the harm already done). Therefore, former or current employees who publicly reveal the identity of targets or sources of the Service can be prosecuted whether or not the information is true and without the Crown having to address this issue at all.

In Section 14, unauthorized communication of special operational information itself is punishable by up to 14 years' imprisonment.

For both of these offences, there is a 'public interest' defence – if an accused can show that information has been disclosed '**for the purpose of disclosing an offence** under an *Act* of Parliament'. The *Act* sets out guidelines that a judge must consider when making his or her judgment; they include: the seriousness of the

offences, the extent of the disclosure, the harm caused by the disclosure and whether the accused resorted to 'other reasonably accessible alternatives' before disclosing the information. In addition, this public interest defence can **only** be relied on if the accused has first (a) advised his or her Deputy Minister (or the Attorney General of Canada) and (b) if this fails, brought his or her concerns to the attention of either the Security Intelligence Review Committee or the Communications Security Establishment Commissioner.

Conclusion

A combination of legislation, government policy and administrative procedures is aimed at preventing and responding to the unauthorized disclosure of government of information, for example, the government Security Policy, oath of office, breach of trust by public officer under the Criminal Code. Prosecution under the *Official Secrets Act* has been, and is, only one response, sometimes referred to as a last resort.

For the first time in over 60 years, the Government has brought in substantive amendments to the *Official Secrets Act*. While part of the Government's anti-terrorism legislation – and therefore seen as part of the Government's response to the events of September 11, 2001 – these amendments, and the issues surrounding them, have a longer history in Canada.

The amendments respond to long-standing criticisms of the *Official Secrets Act* and have been drafted, as all legislation now is, in light of the Charter of Rights and Freedoms. As the Minister of Justice and Solicitor General have said, the new *Security of Information Act* recognizes the reality of 'new players and new threats'.

For current and former employees in the security and intelligence community, there is now a much clearer statement of their responsibilities to safeguard sensitive information – and a much clearer statement of their potential criminal liability should such sensitive information be disclosed without authorization.

Backgrounder Series

No. 12 **February 2002**

Backgrounder Series is produced by Communications Branch. For information on other publications in the series or to obtain more information about CSIS you can visit our Internet web site at: www.csis-scrs.gc.ca, or please call (613) 231-0100 or write to:

CSIS
P.O. Box 9732
Postal Station T
Ottawa, Ontario
K1G 4G4
Attn: Communications Branch

Service canadien du renseignement de sécurité

Série d'aperçus

N° 12
février 2002

Loi sur la protection de l'information

Le Service canadien du renseignement de sécurité est voué à assurer la sécurité nationale et celle des Canadiens. Pour que le SCRS puisse s'acquitter efficacement de cette tâche, il faut absolument que les Canadiens comprennent son mandat. Cette série d'aperçus constitue un moyen économique d'informer le public canadien sur les priorités et les tâches du SCRS ainsi que sur le contexte dans lequel un service du renseignement de sécurité moderne doit évoluer.

Introduction

Dans le présent *Aperçu*, nous essaierons d'expliquer les récentes modifications apportées à la *Loi sur les secrets officiels* - dont le nom a également été changé - afin que les personnes qui pourraient être assujetties à la *Loi*, notamment en raison de leur emploi actuel ou antérieur, soient au courant des nouvelles dispositions. En 1981, la Commission McDonald a signalé que l'une des lois les plus importantes pour le travail d'un service de sécurité est la *Loi sur les secrets officiels*. La Commission de réforme du droit a indiqué que la *Loi sur les secrets officiels* prévoit des crimes qui comptent parmi les infractions criminelles les plus graves puisqu'ils « compromettent la sécurité et le bien-être de l'État canadien et de ses habitants ».

La *Loi antiterroriste* du gouvernement fédéral, soit le projet de loi C-36, devenu le Chapitre 41 des *Lois du Canada (2001)*, a reçu la sanction royale le 18 décembre 2001 et est entrée en vigueur le 24 décembre 2001.

Le projet de loi C-36 est divisé en sept parties de la manière suivante :

Partie 1 : modification du *Code criminel* (56 pages)
Partie 2 : modification de la *Loi sur les secrets officiels* (20 pages)
Partie 3 : modification de la *Loi sur la preuve au Canada* (20 pages)
Partie 4 : *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (22 pages)

Partie 5 : modifications à d'autres lois (dont la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*, la *Loi sur le Service canadien du renseignement de sécurité*, la *Loi sur la défense nationale*) (18 pages)

Partie 6 : *Loi sur l'enregistrement des organismes de bienfaisance (renseignement de sécurité)* (9 pages)

Partie 7 : Dispositions de coordination, de révision et d'entrée en vigueur (37 pages)

Contexte

Au cours des 30 dernières années, la *Loi sur les secrets officiels* a constamment fait l'objet de critiques et d'appels à un remaniement.

La première *Loi sur les secrets officiels* a été votée en Grande-Bretagne en 1889 et promulguée presque textuellement au Canada en 1890. La *Loi* canadienne a été incluse dans le premier *Code criminel* en 1892, dont elle a fait partie jusqu'en 1939, date à laquelle la *Loi sur les secrets officiels* actuelle a été rapidement votée à la veille de la Deuxième Guerre mondiale. Depuis 1939, et jusqu'à ce que le projet de loi C-36 soit voté récemment, aucune modification majeure n'a été apportée à la *Loi*.

La *Loi sur les secrets officiels* de 1939 comportait deux principales dispositions : i) l'article 3, portant sur le délit d'«espionnage », et ii) l'article 4, qui interdisait la « communication illicite de renseignements » (communément appelée « divulgation illicite »). Depuis 1939, il y a eu environ deux douzaines de poursuites, presque toutes en vertu de l'article visant l'espionnage - et il n'y en a eu que six au cours des 40 dernières années. Parmi les cas les plus célèbres, dont ceux où des poursuites n'ont pas été intentées, mentionnons les suivants : Peter Treu (1978), le *Toronto Sun* (1979), Hugh Hambleton (1982), James Morrison (1986), Stephen Ratkai (1989), Brian McInnis (1994-1995).

Au cours des 30 dernières années, on a plus ou moins cherché à améliorer ou à remplacer la *Loi* selon les événements entourant des incidents de divulgation illicite et d'espionnage, les poursuites intentées en vertu de la *Loi*, les recommandations de commissions fédérales et d'autres faits nationaux ou internationaux.

En 1969, la Commission royale d'enquête sur la sécurité (la « Commission Mackenzie ») a décrit la *Loi sur les secrets officiels* comme « une loi inextricable rédigée en termes larges et ambigus »; la Commission a conclu que « l'on devait songer à remanier de fond en comble la *Loi sur les secrets officiels* ».

Au début des années 1970, de nombreux pays démocratiques se sont débattus avec la question de l'amélioration de l'accès du public aux informations gouvernementales. En 1976, la Chambre des communes a renvoyé à un comité mixte permanent les questions concernant l'accès à l'information, la protection de la vie privée et la *Loi sur les secrets officiels*. L'examen des deux premières questions a donné lieu à l'adoption, en 1983, de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, mais la troisième n'a pas reçu la même attention.

En 1979, la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (la « Commission McDonald ») a consacré plus de la moitié de son premier rapport, intitulé *Sécurité et Information*, à examiner la *Loi sur les secrets officiels* et à recommander des modifications de celle-ci. Ces recommandations ont été réitérées dans le deuxième rapport de la Commission McDonald

publié en août 1981, le rapport qui est à l'origine de la décision du gouvernement de créer le SCRS. Toutefois, la *Loi sur les secrets officiels* n'a pas été modifiée, bien que la nécessité d'un remaniement ait été reconnue de façon générale et à maintes reprises.

Enfin, en 1986, la critique peut-être la plus acerbe au sujet de la *Loi sur les secrets officiels* a été formulée par la Commission de réforme du droit dans son *Document de travail 49*. La Commission en est arrivée à la conclusion suivante :

> « Non seulement les infractions actuelles contre l'État sont vieillies, complexes, répétitives, vagues, incohérentes, trop extensives et ne relèvent d'aucun principe, mais tout porte à croire que certaines d'entre elles contreviennent en plus aux dispositions de la *Charte canadienne des droits et libertés* ».

Questions

Même si la *Loi sur les secrets officiels* a fait l'objet de nombreuses critiques, il est reconnu et prouvé que le remaniement de celle-ci est une entreprise ardue.

La tâche est peut-être plus facile dans le cas des dispositions relatives à l'**espionnage** puisqu'il s'agit d'établir quand un citoyen devrait être considéré comme criminellement responsable de la communication d'informations **à une entité étrangère** lorsque cette communication expose de quelque façon le Canada à un danger ou crée un avantage pour cette entité étrangère. D'autres questions se posent à cet égard : quel type d'information devrait être visé? qui sont les « entités étrangères »? qu'est-ce que cela signifie et comment prouver dans un contexte criminel que la communication a été faite « dans le dessein de nuire à la sécurité ou aux intérêts de l'État » (pour reprendre l'expression utilisée à l'article 3 de l'ancienne *Loi sur les secrets officiels*)?

Les dispositions concernant la **divulgation illicite** sont plus problématiques, car elles se rapportent à la communication d'informations non pas à des entités étrangères mais **à qui que ce soit** (journalistes, députés, groupes d'intérêt, etc.). La communication non autorisée d'informations gouvernementales peut nuire autant à la souveraineté d'un État et à la sécurité de ses citoyens que l'espionnage; toutefois, contrairement à l'espionnage, les enjeux ne sont pas toujours évidents, et parfois ils sont même inexistants. La divulgation illicite est vraisemblablement davantage associée à des questions comme la liberté d'expression, l'obligation de rendre compte du gouvernement, la nécessité d'informer le public à propos d'importantes questions de politique publique et la dénonciation.

Plus récemment, mais là-encore avant les événements du 11 septembre 2001 et le projet de loi C-36, le besoin d'examiner la *Loi sur les secrets officiels* s'est de nouveau fait sentir au gouvernement. En 1998, dans sa Déclaration sur la sécurité nationale à la Chambre des communes, le solliciteur général d'alors, Andy Scott, s'est exprimé en ces termes :

> « Dans le cadre des mesures qu'il prend pour contrer les menaces émanant de l'étranger et d'ailleurs, le gouvernement revoit aussi la *Loi sur les secrets officiels*, à laquelle on reproche de manquer de précision, d'être trop générale et de ne pas traiter des questions actuelles de sécurité nationale. Cette loi prenait appui, à l'origine, sur une notion maintenant dépassée de la défense et de la sécurité nationales, associée surtout à la sécurité matérielle et à la protection du pays contre les menaces d'ordre militaire. Aujourd'hui, à l'ère de l'informatique, le

crime, le terrorisme et l'espionnage ne connaissent plus de frontières, et de nouveaux types de menaces peuvent compromettre la souveraineté du Canada. Pour les éliminer, nous devons nous doter d'une législation moderne, précise et claire, qui refléterait les valeurs du Canada d'aujourd'hui. »

La nouvelle Loi sur la protection de l'information

Vue d'ensemble

Dans un communiqué intitulé *Information*, publié le 18 décembre 2001, date à laquelle le projet de loi C-36 a reçu la sanction royale, le gouvernement du Canada a décrit brièvement les modifications apportées à la *Loi sur les secrets officiels* :

> « La *Loi sur les secrets officiels* (a été) modifiée pour répondre aux préoccupations visant la sécurité nationale, y compris les menaces que constituent l'espionnage par des puissances étrangères et des groupes terroristes, et l'intimidation ou la coercition à l'égard de collectivités ethnoculturelles au Canada. La Loi aura également un nouveau titre : *Loi sur la protection de l'information*.
>
> De nouvelles infractions (ont été) créées pour améliorer et moderniser les dispositions portant sur « l'espionnage », en tenant compte des nouvelles réalités, notamment des nouveaux intervenants et des nouvelles menaces. Ces infractions porteront essentiellement sur les situations où il convient que le Canada protège ses institutions et ses citoyens des activités de recherche de renseignements nuisibles ou susceptibles de l'être pour le Canada.
>
> Les nouveaux intervenants, autres que les gouvernements d'États traditionnels, comprennent les gouvernements en attente, les gouvernements en exil et d'autres puissances étrangères, de même que les groupes terroristes.
>
> Les nouvelles menaces reconnues comprennent les menaces contre les collectivités ethnoculturelles au Canada, les menaces aux secrets industriels et les menaces aux infrastructures essentielles, tant publiques que privées.
>
> Le projet de loi prévoit également de nouvelles infractions spéciales ayant trait à la communication non autorisée, ou la prétendue communication, de renseignements opérationnels spéciaux (par exemple, l'identité des sources confidentielles, des agents secrets ou des personnes recherchées par le SCRS) par des personnes astreintes au secret à perpétuité. »

Nouveaux concepts et définitions

Nouveaux intervenants

Tel que noté dans le communiqué intitulé *Information*, la *Loi sur la protection de l'information* comprend de « nouveaux intervenants ». L'ancienne *Loi sur les secrets officiels* prévoyait des infractions relatives à l'espionnage qui comportaient la communication à une « puissance étrangère » (non définie); la nouvelle *Loi* renferme des définitions plus précises des termes « État étranger », « puissance étrangère » (vaste définition englobant les gouvernements d'États étrangers, les quasi-gouvernements et ceux qui aspirent à assumer le gouvernement) et « entité étrangère » (dont la définition englobe des puissances étrangères, des groupes formés de puissances étrangères ou des

personnes agissant en collaboration avec eux ou pour leur profit). La nouvelle *Loi* mentionne également les « groupes terroristes », en intégrant la définition tirée des récentes modifications apportées au Code criminel dans le cadre du projet de loi C-36.

Atteinte aux intérêts canadiens

L'ancienne *Loi sur les secrets officiels* prévoyait une infraction d'espionnage dans les cas où la Couronne pouvait prouver que la communication était effectuée dans « **un dessein** nuisible à la sécurité ou aux intérêts de l'État » (non défini); la nouvelle *Loi sur la protection de l'information*, aux alinéas 3(1)*a*) à *n*), définit cette expression en détail. Ces alinéas prévoient entre autres les cas suivants :

- commettre une infraction, punissable d'une peine d'emprisonnement maximale de deux ans ou plus, en vue de contribuer à la réalisation d'un objectif politique, religieux ou idéologique ou dans l'intérêt d'une entité étrangère ou d'un groupe terroriste;
- se livrer, même à l'étranger, à une activité terroriste (dont la définition est, là aussi, tirée du Code criminel);
- porter atteinte à des services ou à des systèmes, publics ou privés, d'une façon qui nuit gravement à la santé, à la sécurité ou au bien-être économique ou financier de la population canadienne ou au bon fonctionnement d'un gouvernement au Canada (c'est-à-dire, porter atteinte aux infrastructures essentielles du Canada);
- compromettre la puissance militaire des Forces canadiennes;
- compromettre ou menacer la capacité du gouvernement fédéral en matière de sécurité ou de renseignement;
- compromettre ou menacer la capacité d'entretenir des relations diplomatiques ou de mener des négociations internationales.

Pour l'application de la *Loi sur la protection de l'information*, il y a atteinte aux intérêts canadiens dans les cas où l'entité étrangère ou le groupe terroriste se livre à l'une quelconque de ces activités.

Renseignements protégés

La nouvelle *Loi* ne fait pas état d'« informations classifiées », mais renferme plutôt l'expression « renseignements **à l'égard desquels** le gouvernement fédéral ou un gouvernement provincial **prend des mesures de protection** ». Dans cette optique, lors d'une poursuite, la Couronne devra montrer que le gouvernement a pris certaines mesures pour protéger les renseignements. La classification de sécurité serait vraisemblablement un moyen de le démontrer, mais ce n'est pas le seul. Par exemple, si le directeur du SCRS dit à un employé de ne pas divulguer l'endroit à l'étranger où se déroulera une rencontre avec une source humaine, il pourrait s'agir là (si la preuve en est présentée au tribunal) d'un renseignement à l'égard duquel le gouvernement a « pris des mesures de protection ». Ce renseignement serait donc visé par les dispositions de la *Loi sur la protection de l'information* même s'il ne se trouvait pas dans un document classifié.

Renseignements opérationnels spéciaux

Il s'agit ici d'un nouveau concept dans lequel le législateur tente de définir les informations du gouvernement qui sont les plus sensibles sur le plan opérationnel. Les « renseignements opérationnels spéciaux » sont définis comme étant des renseignements à l'égard desquels le gouvernement fédéral prend des mesures de protection et dont la communication révélerait ou permettrait de découvrir des informations sensibles, entre autres :

- l'identité de sources confidentielles d'information ou d'assistance pour le gouvernement du Canada (actuelles ou passées) :
- des lieux, des personnes, des groupes ou des entités au sujet desquels le gouvernement a mené, mène ou entend mener des activités secrètes de collecte de renseignements;
- l'identité de toute personne qui a mené, mène ou pourrait être appelée à mener secrètement ces activités de collecte;
- des plans en vue de certaines opérations militaires;
- les moyens que le gouvernement utilise pour la protection d'information, notamment le chiffrement et les failles de ces moyens;
- des éléments d'information de la nature de ceux susmentionnés, reçus d'une entité étrangère ou d'un groupe terroriste ou le concernant.

Personnes astreintes au secret à perpétuité

Un autre nouveau concept mis de l'avant dans la *Loi* est la description d'individus qui sont assujettis à une norme de responsabilité plus élevée à l'égard de communications non autorisées. Les personnes soumises à ce « régime spécial » sont : (a) les membres ou les employés - anciens ou actuels - d'un ministère ou organisme désigné dans une annexe de la *Loi* ou (b) les personnes nommément désignées par un avis conformément à la *Loi* (et les règlements). Appartiennent à la première catégorie :

- les employés - anciens ou actuels - du SCRS;
- les employés - anciens ou actuels - du Centre de la sécurité des télécommunications;
- les anciens membres ou employés du Service de sécurité de la GRC et de la Direction des communications du Conseil national de recherches du Canada;
- les employés - anciens ou actuels - du Comité de surveillance des activités de renseignement de sécurité et du bureau de l'Inspecteur général du SCRS;
- les employés ou les membres - anciens ou actuels - de certains groupes au sein de la GRC (par exemple, le Programme des renseignements criminels et le Programme des missions de protection).

Infractions

Se fondant sur les définitions et les concepts susmentionnés, la *Loi sur la protection de l'information* prévoit un certain nombre d'infractions relatives à l'espionnage et à la divulgation illicite. Il ne peut toutefois être engagé de poursuites pour ces infractions à la *Loi* sans le consentement du procureur général du gouvernement fédéral. Voici une brève description de ces nouvelles infractions. Pour plus de détails sur ces notions complexes, veuillez consulter la *Loi* proprement dite, qui figure sur le site Web du SCRS, à l'adresse www.csis-scrs.gc.ca.

Espionnage

Est passible de poursuite et de l'emprisonnement à perpétuité quiconque communique à une entité étrangère ou à un groupe terroriste des renseignements s'il sait qu'il s'agit de renseignements protégés ou ne se soucie pas de savoir si tel est le cas, et s'il les communique dans l'intention d'accroître la capacité de ce groupe étranger de porter atteinte aux intérêts canadiens ou ne se soucie pas de savoir si la communication aura cet effet (article 16). De plus, l'article 17 prévoit une infraction spécifiquement applicable à la communication de « renseignements opérationnels spéciaux ». Pour qu'il y ait délit, il n'est pas nécessaire que la personne ait l'intention de nuire; il suffit qu'elle croie que les informations qu'elle communique constituent des renseignements opérationnels

spéciaux ou ne se soucie pas de savoir si tel est le cas. Là encore, la peine prévue peut aller jusqu'à l'emprisonnement à perpétuité.

Une autre disposition nouvelle, l'article 20, traite des personnes qui, sur l'ordre d'une entité étrangère ou d'un groupe terroriste, incitent ou tentent d'inciter une personne à accomplir quelque chose qui portera vraisemblablement atteinte aux intérêts canadiens ou qui vise à accroître la capacité d'étrangers d'y porter atteinte. Encore une fois, la peine maximale prévue pour cet acte est l'emprisonnement à perpétuité.

Autre élément nouveau, « l'espionnage économique » constitue un crime en vertu de la *Loi*. Il s'agit de la communication frauduleuse ou « sans apparence de droit » d'un « secret industriel » (défini) à une « entité économique étrangère » (définie comme étant une « entité qui appartient, en totalité ou pour une partie importante, à un État étranger, ou qui est contrôlée en droit ou de fait » par un État étranger). Cette infraction est passible d'un emprisonnement maximal de dix ans.

Enfin, la *Loi* prévoit un certain nombre d'« actes préparatoires » passibles d'un emprisonnement maximal de deux ans. Ils peuvent comprendre : (a) entrer au Canada sur l'ordre d'une entité étrangère ou d'un groupe terroriste, (b) obtenir l'accès à des renseignements, (c) informer sciemment ces groupes étrangers que l'on est disposé à commettre l'infraction, (d) posséder un instrument ou un logiciel utile pour la dissimulation de la teneur de renseignements, ou pour la communication secrète de renseignements.

Divulgation illicite

La nouvelle *Loi sur la protection de l'information* conserve l'ancienne infraction de communication non autorisée (article 4) de la *Loi sur les secrets officiels*. La plupart des nouvelles infractions prévues ont trait aux « personnes astreintes au secret à perpétuité », ces « initiés » qui sont visés soit en raison de l'endroit où ils travaillent (par exemple, des employés - anciens ou actuels - du SCRS et du CST), soit parce qu'ils ont personnellement reçu un avis en ce sens de leur sous-ministre.

Par exemple, l'article 13 prévoit une infraction - passible d'un emprisonnement maximal de cinq ans - dans le cas d'un initié qui, « intentionnellement et sans autorisation, communique ou confirme des renseignements qui, **s'ils étaient vrais**, seraient des renseignements opérationnels spéciaux ». Cette définition du délit de **prétendue** communication suppose que (a) les initiés sont assujettis à une obligation particulière à l'égard des renseignements les plus sensibles qu'ils ont détenus ou auxquels ils ont accès et que (b) la Couronne n'a pas à prouver la véracité des renseignements (puisque l'expérience a montré que cela ne fait souvent qu'ajouter au tort déjà causé). Par conséquent, les anciens employés ou les employés actuels qui révèlent publiquement l'identité de cibles ou de sources du Service peuvent être poursuivis indépendamment de la véracité des renseignements et sans que la Couronne n'ait à démontrer celle-ci.

En vertu de l'article 14, la communication non autorisée de renseignements opérationnels spéciaux est en soi passible d'un emprisonnement maximal de quatorze ans.

Pour ces deux infractions, la personne accusée peut se défendre en faisant valoir qu'elle a agi dans l'« intérêt public », c'est-à-dire qu'elle a communiqué les renseignements **en vue de**

révéler une infraction à une loi fédérale. La *Loi* énonce les facteurs que le juge doit prendre en considération avant de se prononcer, entre autres, sur la gravité de l'infraction, à quoi se limitait la révélation, le préjudice causé par la révélation et si la personne a utilisé ou non au préalable « les solutions de rechange dont elle pouvait raisonnablement se prévaloir ». De plus, la défense d'intérêt public ne peut être invoquée **que si** la personne a au préalable (a) informé de la question son sous-ministre (ou le procureur général du Canada) et (b) dans l'éventualité où cela n'a pas donné de résultat, elle a fait part de ses préoccupations au Comité de surveillance des activités de renseignement de sécurité ou au commissaire du Centre de la sécurité des télécommunications.

Conclusion

Pour prévenir la communication non autorisée de renseignements du gouvernement et y réagir, il existe tout un éventail de mesures législatives, de politiques gouvernementales et de procédures administratives, comme la politique du gouvernement sur la sécurité, le serment professionnel, l'infraction prévue dans le *Code criminel* pour abus de confiance par un fonctionnaire public. Les poursuites intentées en vertu de la *Loi sur les secrets officiels* n'ont été et ne sont toujours qu'un moyen parmi d'autres et ne sont parfois utilisées qu'en dernier recours.

Pour la première fois en plus de 60 ans, le gouvernement a apporté des modifications de fond à la *Loi sur les secrets officiels*. Même si elles s'inscrivent dans le cadre des mesures législatives antiterroristes du gouvernement - et sont donc considérées comme un élément de la réaction du gouvernement aux événements du 11 septembre 2001 – ces modifications et les questions qui s'y rapportent faisaient l'objet de discussions bien avant cela au Canada.

Ces modifications visent à répondre aux critiques que suscitait depuis longtemps la *Loi sur les secrets officiels* et ont été rédigées, comme le sont maintenant toutes les lois, à la lumière de la *Charte des droits et libertés*. Comme l'ont dit le ministre de la Justice et le Solliciteur général, la nouvelle *Loi sur la protection de l'information* reconnaît la réalité « des nouveaux intervenants et des nouvelles menaces ».

Les anciens employés et les employés actuels de la communauté de la sécurité et du renseignement disposent maintenant d'un énoncé beaucoup plus clair de leurs responsabilités à l'égard de la protection d'informations sensibles, ainsi que de leur éventuelle responsabilité criminelle en cas de communication non autorisée de ces informations.

Série d'aperçus

février 2002 **N° 12**

Série d'aperçus est préparée par la Direction des communications. Pour de plus amples renseignements sur les publications de cette série, ou pour obtenir plus d'informations à propos du SCRS, vous pouvez visiter notre site internet au : www.csis-scrs.gc.ca. Il est également possible de nous rejoindre par téléphone au (613) 231-0100 ou écrire à :

SCRS
Case postale 9732
Succursale T
Ottawa (Ontario)
K1G 4G4
À l'att. de : Direction des communications